UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/006,554	12/06/2001	Farshid Sabet-Sharghi	250543-31500	2639

69735 7590 01/23/2008
WINSTON & STRAWN, LLP
PATENT DEPARTMENT
1700 K STREET, N.W.
WASHINGTON, DC 20006

EXAMINER	
GELAGAY, SHEWAYE	
ART UNIT	**PAPER NUMBER**
2137	
MAIL DATE	**DELIVERY MODE**
01/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/006,554	**Applicant(s)** SABET-SHARGHI ET AL.	
	Examiner Shewaye Gelagay	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 11/8/07.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 4,6,7 and 24-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 4,6-7 and 24-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date 7/24/07, 9/18/07.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 7/24/07 has been entered.

Election/Restrictions

2. Applicant's election without traverse of Group I (claims 4, 6-7 and 24-29) in the reply filed on 11/8/07 is acknowledged. The examiner would like to point out applicant has listed the elected claims as 4-6, 7 and 24-29 in the reply filed 11/8/07. However, claim 5 is canceled; claims 4, 6-7 and 24-29 not claims 4-6, 7 and 24-29 are included in Group I.

3. Claims 4, 6-7 and 24-29 are pending.

Response to Arguments

4. Applicant's arguments filed 7/24/07 have been fully considered but they are not persuasive. In response to the applicants argument the following comments are made:

The applicant argued that Hirota is silent on the quantity of content (measured in a decrypted and decoded format) that is copied and decrypted before copying and decrypting an additional quantity. Hirota teaches hierarchical data structure of an AOB file (hereinafter file), the first level shows file, second level audio object AOB (AOB) itself, the third level shows AOB-Block (hereinafter Block), the fourth level and AOB_ELEMENT (hereinafter Element), and the fifth level an AOB_FRAME(`hereinafter Frame) . The Frame is the smallest unit composed of audio data in ADTS format and ADTS header encoded according to MPEG2-ACC standard, encrypted, transmitted and can be played back. The audio data length in each Frame is restricted to a playback time of only 20ms. An Element is a group of consecutive Frames, the number of Frames in an Element depends on the value set at the sampling frequency is set so that the total playback time of the Frames will be around two seconds. BLOCK is composed of valid Elements and only one Block exists in each File. While an Element has a playback period of around two seconds, Block has a maximum playback period of 8.4 minutes (col. 14, lines 4-67)

Hirota teaches an audio track including a plurality of encrypted AOBs encrypted with a plurality of different encryption keys. When an audio stream is for a music album which includes a long track, the long track is divided into a plurality of files to ensure that the number of pieces of entry information for a single file does not exceed a predetermined number. When a playback apparatus reads a file and commences playback of AOBs included in the file, the playback apparatus also reads the management information and stores it in internal memory. When the playback of this AOB ends, the following AOB is read and overwritten into the internal memory of the payback apparatus to take place the management information that was hitherto stored. (col. 3, line 65-col. 5, line 40)

The output of the Frame and overwriting the cluster data are repeatedly performed, so that the Frames included in the File are successively outputted to the descrambler and AAC decoder. (col. 43, lines 40-67) The playback apparatus accesses the authentication region and reads the FileKey that is stored having the same number as the File. The FileKey is sent to the descrambler, so that by successively outputting Frames included in the File into the descrambler the Frames can be successively played back. (i.e. copying a fractional portion of encrypted audio or video content of the file, the fractional portion comprising less than about 10 seconds of content of the file) (col. 44, lines 10-49)

Therefore Hirota teaches that a file is descrambling and decryption each File with different key. Each file comprises minimum playback of two seconds and maximum playback of 8.4 minutes. (i.e. the quantity of content copied and decrypted before copying and decrypting an additional quantity)

The applicant argued that Examiner has recently asserted the term "track" refers to a meaningful payback unit for users and would lead one of skill in the art to decrypt an entire track at once, once the proper keys are calculated or decrypted and therefore made ready for use in such process. The Examiner would like to point out again, Hirota teaches an audio track including a plurality of encrypted AOBs encrypted with a plurality of different encryption keys. When an audio stream is for a music album which includes a long track, the long track is divided into a plurality of files to ensure that the number of pieces of entry information for a single file does not exceed a predetermined number. When a playback apparatus reads a file and commences playback of AOBs included in the file, the playback apparatus also reads the management information and stores it in internal memory. When the playback of this AOB ends, the following AOB is read and overwritten into the internal memory of the payback apparatus to take place the management information that was hitherto stored. (col. 3, line 65-col. 5, line 40) Applicant also teaches "Each track may be made of multiple files, for example, in case of a long classical song. For large video clips, a title may comprise many files." Therefore a track is not decrypted in its entirety instead the track is divided into a plurality of files which are descrambled and decrypted with different keys.

The applicant argued that nothing within Hirota and Tagawa teaches one to delete media unique key part way through decrypting a track. The media unique key once calculated is needed to decrypt the rest of the track, and it would be counter intuitive to decrypt it before the track is decrypted. The situation with the title key is similar as an appropriate and decrypted title key or keys are also needed to decrypt the track. Hirota teaches the FileKey (i.e. title key) is encrypted using any value obtained by subjecting the media ID stored in the special region into a predetermined calculation can be used to encrypt the FileKey. (which is consistent with the applicant teaching of calculating media unique key and decrypting the title key with the media unique key) Applicant teaches "the media key Km and the media Identifier IDmedia are combined by use of a C2 one-way function to produce the media unique key Kmu"

Hirota teaches data can only be read from or written into the authentication region if mutual authentication has been successfully performed by the flash memory card and the device connected to the flash memory card. (col. 10, lines 3-35)The

FileKeys are stored in the authentication region. (col. 13, lines 22-28) The playback apparatus that has succeeded in obtaining secure media ID then performs mutual authentication with the authorization unit of the flash memory card. When the mutual authentication succeeded, the payback apparatus generates a command for accessing the authentication region of the flash memory card ..., the authentication region access control unit accesses the sector specified by the valid parameters and reads the encryption key FileKey and encrypts the encryption key FileKey using the secure key obtained during the mutual authentication...the playback apparatus decrypts the encryption key FileKey using the secure key...and decrypt again the encryption FileKey using the master key and the media ID to obtain the encryption key FileKey. Once the encryption key FileKey has been obtained and an AOB corresponding to this encryption key FileKey has been read from the obtained authentication region, the AOB is decrypted using the encryption key FileKey and music is simultaneously played. (col. 58, line 50-col. 60, line 13) Therefore the keys are calculated to decrypt and play only an AOB file not the entire track. Hirota further teaches once the playback of

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 4, 6-7 and 24-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hirota et al. (hereinafter Hirota) U.S. Patent 6,856,431 in view of Dolan et al. (hereinafter Dolan) US 5,604,801.

As per claim 4:

Hirota teaches a computer readable storage medium having an executable Program, the program to be utilized in an audio and/or video device for playback of encrypted audio and/or video files, the program configured to:

decrypt encrypted audio and/or video content of the file from a memory card based on a command received from a user interface of the device, (col. 42, lines 34-40) wherein decrypting the audio or video content comprises:

copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device; (col. 59, lines 55-56)

copying a fractional portion of encrypted audio or video content of the file, the fractional portion comprising less than about 10 seconds of content of the file, from the memory card into a memory buffer of the devices; (col. 10, lines 24-25; col. 14, lines 4-67; col. 44, lines 10-49; col.59, lines 65-66, col. 60, lines 5-6; While an Element has a playback period of around two seconds, Block has a maximum playback period of 8.4 minutes)

decrypting one or more of the copied encrypted keys; (col. 10, lines 24-25; col. 58, line 50-col. 60, line 13) decrypting the fractional portion of copied encrypted audio or video content of the file with the one or more decrypted keys; (col. 42, lines 34-35; col. 60, line 11; col. 58, line 50-col. 60, line 13)

In addition, Hirota further discloses when the playback of audio objects which create audio tracks ends, the following audio object is read and when the playback of the following audio object commences, the corresponding management information is read and overwritten into the internal memory of the playback device to take the place of management information that was hitherto stored. (Col. 5, lines 34-39; Col. 20, lines 52-61)

Hirota does not explicitly disclose immediately deleting the one or more keys after decrypting the audio and/or video content before decrypting. Dolan in analogous art, however, discloses immediately deleting the one or more keys after decrypting the audio and/or video content before decrypting. (Abstract; col. 4, lines 50-58) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota with Dolan in order to minimize the damage caused by the exposure of one of the encryption keys. (col. 4, 17-19; Hirota)

As per claim 6:

The combination of Hirota and Dolan teaches all the subject matter as discussed above. In addition, Hirota further discloses a software program wherein about two seconds of content is decrypted at a time with the one or more decrypted keys before the one or more keys are deleted. (col. 15, lines 45-53)

As per claim 7:

Hirota teaches a computer readable storage medium having an executable program, the program to be utilized in an audio and/or video device for playback of encrypted audio/or video content, the program configured to:

decrypt and encrypted audio or video track from the memory card, wherein decrypting the audio or video track comprises:

(a) calculating a media unique key; (Col. 10, lines 26-29; Col. 57, lines 63-65; ; col. 58, line 50-col. 60, line 13) and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; (Col. 10, lines 24-25; col. 58, line 50-col. 60, line 13) and thereafter

(c) decrypting a group of frames comprising a portion of the track less than the entire track; (col. 3, line 65-col. 5, line 40; Col. 42, lines 34-35; col. 58, line 50-col. 60, line 13)

(f) repeating (a) through (e) until the entire track is completed. (col. 20, lines 56-61; Col. 47, lines 25-27; Col. 60, lines 11)

In addition, Hirota further discloses when the playback of audio objects which create audio tracks ends, the following audio object is read and when the playback of the following audio object commences, the corresponding management information is read and overwritten into the internal memory of the playback device to take the place of management information that was hitherto stored. (Col. 5, lines 34-39; Col. 20, lines 52-61)

Hirota does not explicitly disclose (d) deleting the decrypted title key; and (e) deleting the media unique key. Dolan in analogous art, however, discloses the title and disc key may be deleted whenever copying is performed. (Abstract; col. 4, lines 50-58) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota with Dolan in order to minimize the damage caused by the exposure of one of the encryption keys. (col. 4, lines 17-19; Hirota)

As per claim 24:

Hirtota teaches a method for allowing a device having a processor and random access memory to easily access encrypted data from a memory card with a group of commands, the method comprising:

retrieving playlist information from the memory card and storing the information in the random access memory of the device; (col. 44, lines 21-34)

retrieving track information from the memory card and storing the track information into the random access memory of the device; (Col. 20, lines 52-54; Col. 42, lines 34-35; Col. 60, lines 10-11)

receiving a command selected from the group of commands from the device, the command accessing both of the playlist information, and track information from the random access memory; (col. 59, line 53-col. 60, line11) and

executing the command by retrieving the encrypted data stored within the memory card and decrypting the data based on the accessed information, (col. 10, lines 24-25; col.59, lines 55-66, col. 60, lines 5-6) wherein decrypting the data comprises,

(a) calculating a media unique key; (Col. 10, lines 26-29; Col. 57, lines 63-65; col. 58, line 50-col. 60, line 13) and thereafter

(b) decrypting a title key stored in the memory of the device with the media unique key; (Col. 10, lines 24-25; col. 58, line 50-col. 60, line 13) and thereafter

(c) decrypting a group of frames comprising less than an entire track; (col. 3, line 65-col. 5, line 40; Col. 42, lines 34-35; Col. 60, lines 10-11) and thereafter

(f) repeating (a) through (e) until the entire track is completed. (col. 20, lines 56-61; Col. 47, lines 25-27; Col. 60, lines 11)

In addition, Hirota further discloses when the playback of audio objects which create audio tracks ends, the following audio object is read and when the playback of the following audio object commences, the corresponding management information is read and overwritten into the internal memory of the playback device to take the place of management information that was hitherto stored. (Col. 5, lines 34-39; Col. 20, lines 52-61)

Hirota does not explicitly disclose (d) deleting the decrypted title key; and (e) deleting the media unique key. Dolan in analogous art, however, discloses the title and disc key may be deleted whenever copying is performed. (Col. 8, 56-61; Col. 11, lines 32-33) Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the method disclosed by Hirota with Dolan in order to minimize the damage caused by the exposure of one of the encryption keys. (col. 4, lines 17-19; Hirota)

As per claim 25:

The combination of Hirota and Dolan teaches all the subject matter as discussed above. In addition, Hirota further discloses a method wherein the playlist information comprises:

the name of a playlist; (Col. 17, line 39-col. 18, line 67)

the playlist name string length; (Col. 17, line 39-col. 18, line 67)

the playback time of the playlist; (Col. 17, line 39-col. 18, line 67)

the tracks comprised by the playlist; (Col. 17, line 39-col. 18, line 67) and

the index corresponding to the playlist. (Col. 17, line 39-col. 18, line 67)

As per claim 26:

The combination of Hirota and Dolan teaches all the subject matter as discussed above. In addition, Hirota further discloses a method wherein the track information comprises:

a track number; (Col. 17, line 39-col. 18, line 67)

an index corresponding to the track number; (Col. 17, line 39-col. 18, line 67)

a number of track units in the track; (Col. 17, line 39-col. 18, line 67) and

the playback time of the track. (Col. 17, line 39-col. 18, line 67)

As per claim 27:

The combination of Hirota and Dolan teaches all the subject matter as discussed above. In addition, Hirota further discloses a method wherein the track information comprises:

a format type of a track; (Col. 17, line 39-col. 18, line 67)

a sampling frequency of the track; (col. 54, lines 59-63) the size of the track in bytes; (Col. 17, line 39-col. 18, line 67) and

the current track being decrypted. (Col. 17, line 39-col. 18, line 67)

As per claim 28:

The combination of Hirota and Dolan teaches all the subject matter as discussed above. In addition, Hirota further discloses a method wherein the general track information comprises:

the number of audio objects comprised by the track; (figure 16)

the first audio object comprised by the track; (figure 16)

the last audio object comprised by the track; (figure 16)

the current audio object being decrypted; (Col. 42, lines 34-35; Col. 60, lines 10-11) and

the offset of the current audio object. (col. 21, lines 7-13)

As per claim 29:

The combination of Hirota and Dolan teaches all the subject matter as discussed above. In addition, Hirota further discloses a method wherein decrypting the data comprises:

copying one or more encrypted keys from a protected area of the memory card into a memory buffer of the device; (col. 59, lines 55-56)

copying encrypted audio or video content.from the memory card into a memory buffer of the device; (col. 10, lines 24-25; col.59, lines 65-66, col. 60, lines 5-6)

decrypting one or more of the copied encrypted keys; (col. 10, lines 24-25; col.59, lines 65-66, col. 60, lines 5-6) decrypting the copied encrypted audio or video content with the one or more decrypted keys. (col. 42,lines 34-35; col. 60, line 11)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shewaye Gelagay whose telephone number is 571-272-4219. The examiner can normally be reached on 8:00 am to 5:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shewaye Gelagay SG

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

1/20/08